

Exhibit A

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- (b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.
- (c) These Clauses apply to the processing of personal data as specified in Annex II.
- (d) Annexes I to IV are an integral part of the Clauses.
- (e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

- (a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- (b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

- (a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

- (c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

Docking clause

- (a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.
- (b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
- (c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1. Instructions

- (a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
- (b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

- (a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.
- (b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
- (c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
- (d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

- (a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.
- (b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

- (d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
- (e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

- (a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
- (b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

- (a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.
- (b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions
- (c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
 - (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
 - (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

- (3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
 - (4) the obligations in [OPTION 1] Article 32 Regulation (EU) 2016/679/ [OPTION 2] Articles 33, 36 to 38 Regulation (EU) 2018/1725.
- (d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

- (a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- (b) in obtaining the following information which, pursuant to [OPTION 1] Article 33(3) Regulation (EU) 2016/679/ [OPTION 2] Article 34(3) Regulation (EU) 2018/1725, shall be stated in the controller's notification, and must at least include:
 - (1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (2) the likely consequences of the personal data breach;
 - (3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- (c) in complying, pursuant to [OPTION 1] Article 34 Regulation (EU) 2016/679 / [OPTION 2] Article 35 Regulation (EU) 2018/1725, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

- (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- (b) the details of a contact point where more information concerning the personal data breach can be obtained;
- (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under [OPTION 1] Articles 33 and 34 of Regulation (EU) 2016/679 / [OPTION 2] Articles 34 and 35 of Regulation (EU) 2018/1725.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

- (a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
- (b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
 - (1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
 - (2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
 - (3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
- (d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I LIST OF PARTIES

Controller(s): *[Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]*

1. Name: FTX EU Ltd.

23 Spyrou Kyprianou Protopapas Building 3rd floor 4001, Limassol, Cyprus

represented by:

Martha Lambrianou, CEO

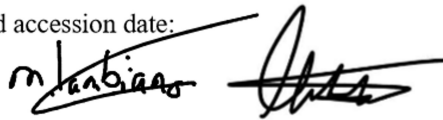
martha@ftx.com

Marios Athinodorou- ED

marios@ftx.com

Signature and accession date:

25.05.2023



Processor(s): *[Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer]*

1. Name: Alvarez and Marsal North America LLC

Address: 2100 Ross Avenue, 21st Floor, Dallas, TX 75201

Contact person's name, position and contact details:

Ed Mosley, Managing Director

emosley@alvarezandmarsal.com

Signature and accession date: ...



ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

Customer data provided by FTX EU Ltd

Categories of personal data processed

General personal data, including but not limited to name, email, bank account numbers

Identification numbers

Bank data

Nature of the processing/ Purpose(s) for which the personal data is processed on behalf of the controller

Collecting, storing, organizing and using as necessary for:

Data preservation – collect, organize and store historical customer data

Customer funds return process – supporting analysis relating to the return of customer funds

As necessary to establish, exercise or defend a legal claim

For the avoidance of doubt, (i) the above limitation of purpose is limited to data constituting personal data within the meaning of Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725 and (ii) all other data may, in addition, be processed to provide any of the services defined as the “Business Purpose” in the amendment to the Engagement Letter, dated as of November 9, 2022, as approved by the Order Authorizing the Retention and Employment of Alvarez & Marsal North America, LLC as Financial Advisors to Debtors and Debtors in Possession pursuant to Sections 327(a) and 328 of the Bankruptcy Code Nunc Pro Tunc to the Petition Date.

Duration of the processing

Continuous for the duration that Services are provided under the Engagement Letter or until terminated (see Clause 10 for termination provisions)

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

See Annex III

Additional business terms

With respect to Clause 7.6(c) and 7.6(d) of the Clauses, controller and processor agree: processor shall, upon request (i) make available to controller all information necessary to demonstrate compliance with Regulation (EU) 2016/679, and (ii) no more than once per calendar year, upon reasonable notice (not less than thirty (30) days) and subject to processor’s onsite safety and security policies and appropriate confidentiality terms between processor and controller, permit and contribute to audits of the processing activities contemplated by these Clauses. Controller may choose to conduct the audit by itself or mandate an independent,

accredited third-party auditor provided that, in processor's reasonable opinion, such auditor is not a competitor of processor. Neither controller nor the auditor shall have access to any data from processor's other customers or to processor systems or facilities not involved in providing the Services.

ANNEX III:

Technical and organisational measures including technical and organisational measures to ensure the security of the data

See next page

ANNEX III - TECHNICAL AND ORGANIZATIONAL MEASURES



Alvarez & Marsal

Security Overview

Last Updated: February 2022

NORTH AMERICA EUROPE MIDDLE EAST LATIN AMERICA ASIA

1. OVERVIEW

At Alvarez & Marsal (A&M), we understand our role as trusted stewards for our clients' most important and valuable assets: their data. A&M's Cybersecurity Program employs a layered, defense-in-depth strategy to protect information assets and systems. Core pillars of this Program include Data Governance, Boundary Defense, Access Control, Endpoint Security, Threat Prevention/Monitoring, Vulnerability Management, Business Continuity, Physical Security, and enterprise-wide Security Awareness. These safeguards, along with a dedicated security function have been implemented to ensure the confidentiality, integrity, and availability of A&M and client data.

The ISO27001 standard informs and supports security related objectives, policies, and procedures including:

- Access control and management
- Security event and access monitoring
- Information system monitoring
- Network intrusion detection
- Network perimeter firewalls
- 2-factor authentication
- Physical and environmental protection
- Contingency planning
- Backup and recovery
- Media handling and protection
- Vulnerability assessment
- Patch management
- Personnel screening
- Configuration management
- Change management
- Transmission encryption
- Malicious code protection
- Audit review, analysis, and reporting
- Security awareness and training
- Controlled system maintenance

Sub-processors of A&M are subject to the firm's Third Party Vendor Risk Management process, whereby security is evaluated for appropriate safeguards relative to the data processed.

1.1. Boundary Defense

Respective of perimeter protection, next-generation Firewalls and Intrusion Detection/Prevention Systems are utilized along the network edge to filter/block malicious and non-standard traffic. Access to Internet domains are further filtered based upon threat indices (e.g. known bad) and reputational factors. Emails entering A&M's network are scanned using multiple layers of technologies for malware, and to proactively detect and block phishing attempts. Further validation of A&M's external posture is determined through a combination of internal and external vulnerability scanning, external penetration testing, and through the use of an independent third-party security scorecard/ratings platform which continuously scans the network edge for security indicators including but not limited to botnet infections, spam propagation, malware, open ports, and TLS/SSL certificates/configuration.

1.2. Endpoint Protection

Careful consideration has been placed on securing the endpoint and thus protecting the information of our clients. Firm laptops are configured with whole disk encryption (encryption at rest), ensuring all content on the disk is encrypted utilizing industry standard AES symmetric encryption. Login to the laptop requires directory-based authentication. Laptops are further hardened to include A&M's security stack, inclusive of local firewall configuration, anti-virus (with

automatic updates), next-generation malware protection (advanced sandboxing, continuous analysis, malware blocking), and DNS layer content filtering functional on and off the corporate network. Security patches are applied in a consistent, timely manner reviewed by A&M's Security Operations team to determine risk and applicability. Data residing on the endpoint is backed-up centrally several times per day, preventing data loss.

1.3. Secure Data Transmission & Storage

A&M recognizes the importance of providing a secure collaborative workspace for information. When agreed-upon with the client, A&M can provide the use of a cloud-based "data room", purpose built to facilitate secure collaboration enforcing both encryption at rest (AES) and in transit (TLS). Client data is logically separated, with access strictly controlled at the file/folder level backed by detailed audit logs. Data backups are encrypted. Where appropriate, Multi-factor Authentication and Information Rights Management (file-level encryption, monitoring, tracking, and near real-time access revocation) capabilities are also utilized. With flexibility in mind, A&M can also support SFTP for bulk transfers or will utilize the technology platforms as provided/required by the client.

1.4. Security Monitoring & Incident Response

Core to A&M's Security Program is the continuous monitoring of security data to identify and quickly respond to potential cyber threats. A&M utilizes industry-leading tools to identify security vulnerabilities followed by analysis and timely remediation. Dark web threat intelligence provides A&M early warning signals to prevent account compromise. Log data from A&M's security stack is centrally collected and managed within a Security Information and Event Management (SIEM) platform. This platform along with others, is monitored 24/7 by A&M's Security Operations Center (SOC) function; a global team comprised of seasoned Security professionals. A&M's Security Incident Response Plan establishes the framework governing the response lifecycle through Identification, Containment, Eradication & Recovery.

1.5. Security Awareness

Supported by firm leadership, Security Awareness Training (covering cyber hygiene) is provided to all employees as part of the on-boarding process and annually thereafter. In addition, periodic messaging and training content is delivered to all workforce members based upon the current cyber threat landscape. When working with especially sensitive and/or regulated data, additional security training may be provided (e.g. HIPAA training).

1.6. Physical Security

Physical security is supported by the use of badge access readers within A&M corporate offices, whereby compartmentalized areas are restricted to authorized personnel. A combination of CCTV/cameras, visitor logs, and capabilities coordinated with building management are utilized. At the user-level, employees are provided with privacy screens to ensure data is protected from public view.

1.7. Data Center Security

A&M utilizes three geographically dispersed co-located data centers. These data center partners have obtained control reporting standard certifications and have undergone independent security

audits from leading financial services and technology companies. These certifications, renewed annually, guarantee that the highest levels of security, availability, integrity and confidentiality controls are continuously maintained within each of A&M's hosted data center environments.

Co-location Partner	Certifications
Digital Realty (Dallas, TX)	ISO 27001, 14001, 9001 PCI DSS SOC 2 SOC 3
QTS (Piscataway, NJ)	ISO 27001 SOC 1 SOC 2 PCI DSS HITRUST
Digital Realty (London, UK)	ISO 27001, 14001, 18001, 50001 SOC 2 Type 2 PCI DSS

Each of A&M's dedicated co-located data centers utilizes an array of security equipment, techniques, and procedures to control, monitor, and record access to the facility, including customer cage areas. All areas of A&M's data centers are monitored and recorded using CCTV, and all access points are controlled. Each data center is staffed with 24-hour security officers; visitors are screened upon entry to verify identity, and are escorted to authorized locations based on access permissions controlled exclusively by A&M personnel. Full access history is recorded and is available for audit by A&M and its clients.

A&M's co-located data centers includes the following security and environmental features:

- 24x7x365 security staff
- Biometric readers
- Kinetic and key locks on closed cabinets
- Colocation and critical data center areas have windowless exteriors
- CCTV digital camera coverage of the entire center, including cages, with detailed surveillance and audit logs
- N+1 redundant power
- Uninterruptible Power Supply to prevent power spikes, surges, and brownouts
- Redundant backup diesel generators
- Temperature and humidity control
- Fire detection and suppression
- Visitor access controls

1.8. Business Continuity

A&M employs a dynamic approach to continuity management, with a focus on incident-time decisioning and response by key stakeholders including executive leadership. A&M's workforce is highly mobile supported by technologies facilitating a "work from anywhere" strategy. Client data residing on A&M endpoints are safeguarded from data-loss through automated back-up. All co-located data centers are designed to withstand severe weather and other regional risks purpose built for redundancy with established fail over procedures. A&M has established a Business Continuity framework to support business resiliency, consisting of:

- Business Continuity Plan – Establishes the framework and procedures to "Keep the Business in business until business operations return to normal."
- IT Disaster Recovery Procedures – To recover data and systems within appropriate timeframes.

2. CONFIDENTIALITY

Applying the concept of least privilege, A&M takes a variety of steps to limit access to client data to only those individuals authorized to access this data by virtue of their delivery role. A&M's standard client engagement letter includes formal provisions addressing confidentiality requirements for all data and information received by our clients. For most engagements, client-specific electronic data rooms and project folders are established and maintained throughout the project's life, limiting access to authorized individuals with necessary and defined roles in support of the engagement. These individuals are instructed in advance of their involvement regarding all engagement-specific confidentiality requirements.

2.1. HIPAA/HITECH Compliance

For engagements where electronic protected health information (ePHI) may be stored in electronic form by A&M, as a business associate A&M is required to comply with relevant provisions of the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, and related HIPAA Security Rule, which govern the administrative, physical and logical safeguards associated with protecting ePHI. A&M has implemented the necessary policies, procedures and controls to comply with all HIPAA-HITECH security requirements.



ANNEX IV: LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Sub-processor (Name / Address / Contact)	Description of the processing
Microsoft Corporation 1 Microsoft Way Redmond, WA 98052 USA	Microsoft provides cloud services including Email (via Office 365), Storage (via OneDrive, Azure), and collaboration (via Teams).
Mimecast North America, Inc. 480 Pleasant Street, Watertown, MA 02472 USA	Mimecast provides email security services with its platform also providing for email backup and disaster recovery capability.
Box Inc. 900 Jefferson Avenue, Redwood City, CA 94063 USA	Box is utilized for file storage and secure collaboration.
Alvarez & Marsal Holdings, LLC 600 Madison Avenue New York, NY 10022 USA	A&M affiliates/internal technology providers.
Amazon Web Services, Inc. 410 Terry Ave North Seattle, WA 98109 USA	AWS provides cloud based infrastructure and hosting services including Databases (via RDS), Servers (via EC2), File storage (via S3) and other related services.